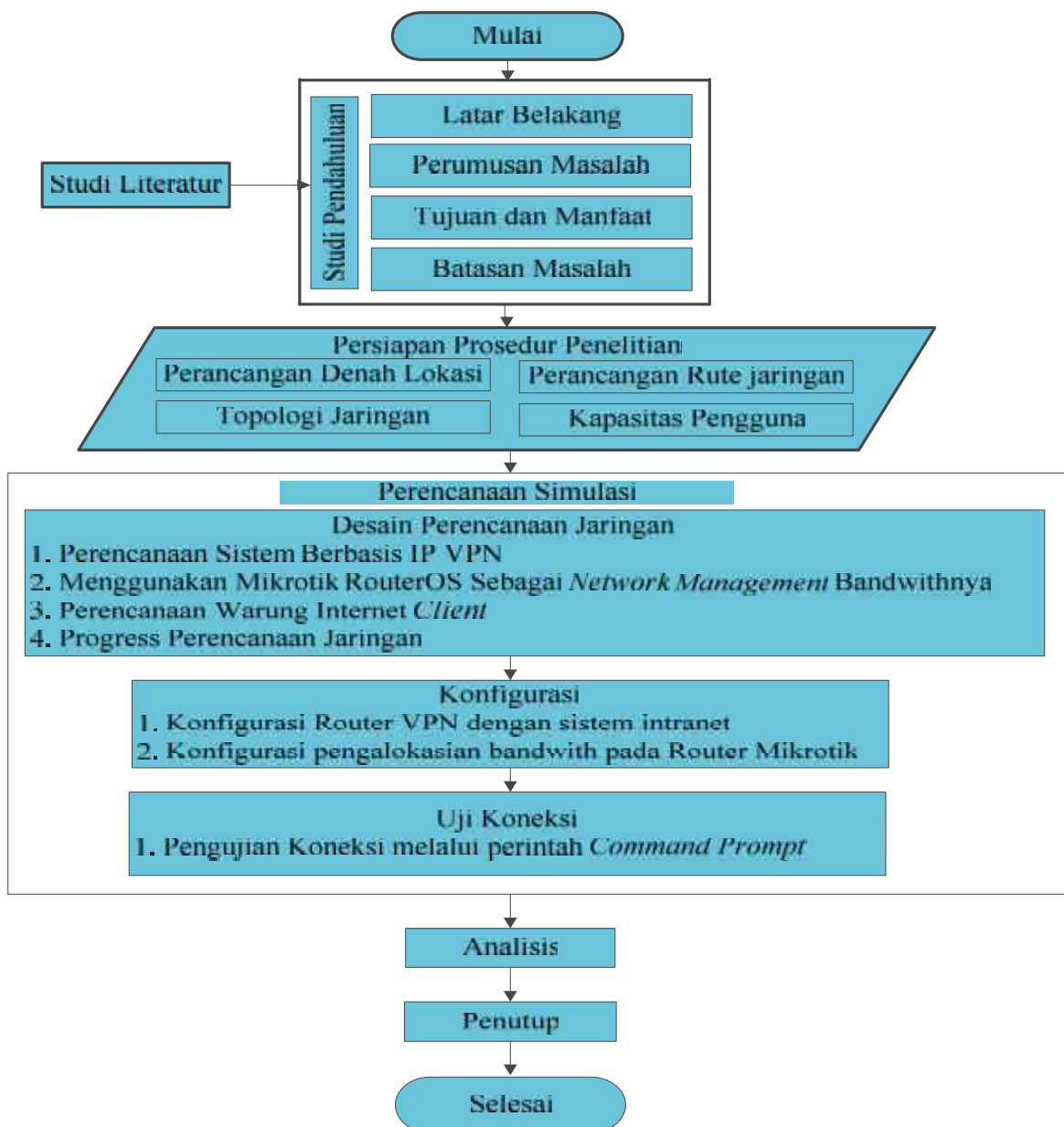


BAB III

METODOLOGI PENELITIAN

Penelitian mengenai perencanaan *internet protocol virtual private network* (IP VPN) dan *network management* untuk efisiensi koneksi internet dengan sistem intranet menggunakan penelitian terapan (*Applied Reseach*) karena dalam pembahasan peneliti berupaya memberikan gagasan baru cara mencapai efisiensi maksimal dalam sebuah perencanaan jaringan internet di sebuah wilayah yang cukup luas. Metodologi penelitian dilakukan sesuai dengan *Flowchart* Gambar 3.1 berikut.



Gambar 3.1 *Flowchart* Metodologi Penelitian

3.1 Studi Pendahuluan

Tahap ini sangat perlu untuk dilakukan yaitu untuk mempermudah mendapatkan dan menemukan permasalahan, tujuan, manfaat serta batasan-batasan yang akan akan diteliti. Adapun cara-cara melakukan studi pendahuluan adalah dengan melakukan survei lapangan langsung yang dalam hal ini di desa Pujud Rokan Hilir Riau dengan cara melihat bagaimana perkembangan internet di desa tersebut dan menyesuaikan keadaan rill lapangan dengan teori penelitian yang telah diperoleh sebagai pembanding proses analisis dan perencanaan.

3.2 Perumusan Masalah

Tujuan dari perumusan masalah ini untuk memperjelas tentang masalah yang akan diteliti dan dibahas dalam penelitian ini. Dari identifikasi masalah maka didapatlah suatu permasalahan yaitu bagaimana merencanakan *Internet Protocol Virtual Private Network* (IP VPN) dan *Network Management* untuk Efisiensi Koneksi Internet dengan Sistem Intranet (Studi Kasus : 4 Warung Internet di Desa Pujud Rokan Hilir Riau).

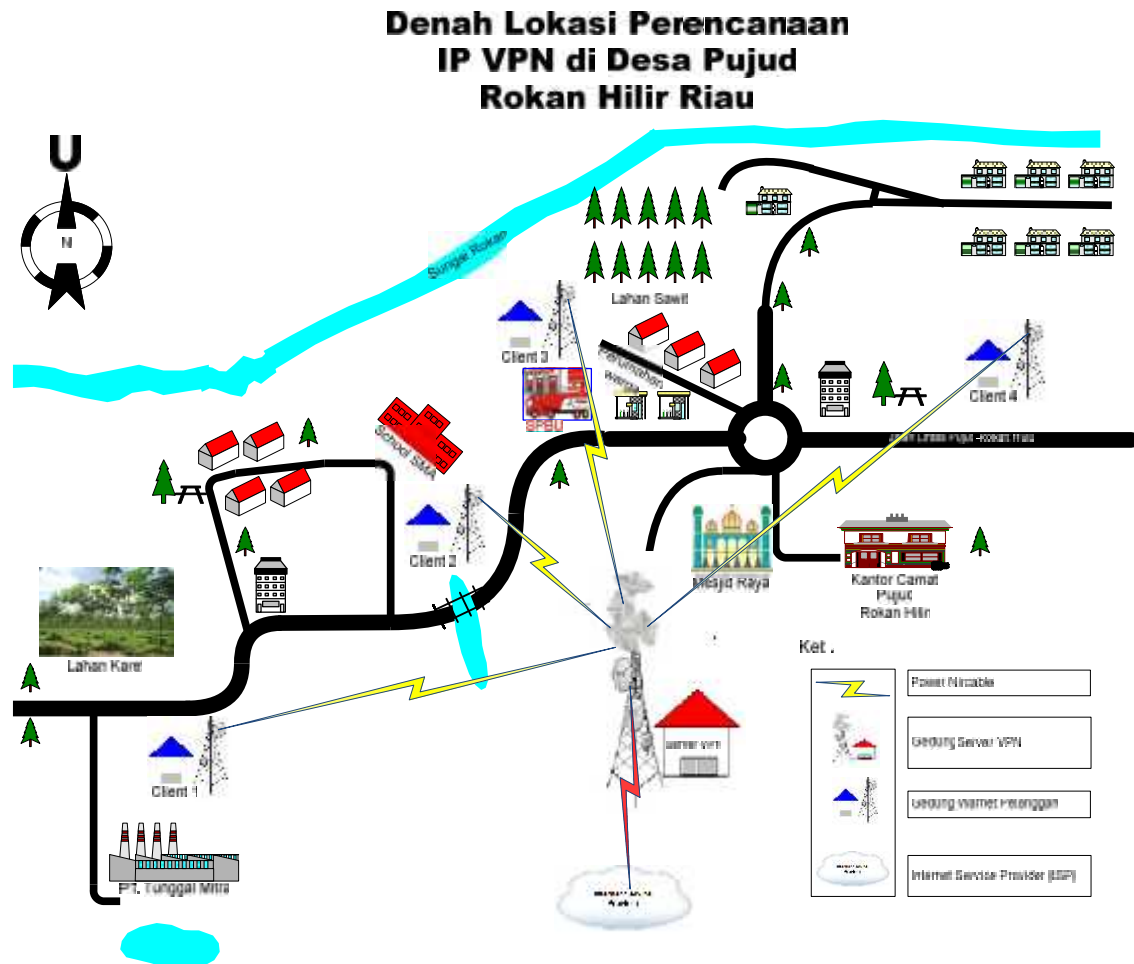
3.3 Studi Literatur

Langkah selanjutnya dalam penelitian ini adalah dengan studi literatur yang berkaitan dengan teknologi jaringan komputer khususnya IP VPN dan *network manajemen*. Referensi dapat diperoleh melalui Perpustakaan Jurusan, Fakultas, maupun Universitas. Informasi dari internet yang akurat dan terpercaya juga dapat dijadikan referensi. Pengambilan data di lapangan juga dilakukan guna menyesuaikan keadaan rill lapangan dengan teori penelitian sebagai bahan penelitian. Tahap ini dilakukan bertujuan untuk mendapatkan referensi-referensi atau literatur-literatur yang bisa mendukung dalam pemecahan permasalahan yang ada.

3.4 Persiapan Prosedur Penelitian

3.4.1 Perencanaan Denah Lokasi

Dalam perencanaan suatu jaringan maka perlu dilakukan perencanaan rute jaringan sesuai dengan kondisi di lapangan, maka dilakukanlah perencanaan denah lokasi tersebut. Untuk penempatan warung internet (warnet) disesuaikan dengan lokasi yang memiliki potensi memadai sebagai pendukung pembuatan warnet seperti pada Gambar 3.2 berikut.



Dari gambar 3.2 maka perencanaan warnet dapat dideskripsikan sebagai berikut :

1. *Client 1* akan di tempatkan di dekat PT Tunggal Mitra, disini merupakan tempat cukup berpotensi untuk di buat warnet, karena nantinya bisa memudahkan bagi para karyawan untuk mengakses internet.
2. *Client 2* akan ditempatkan di dekat Sekolah Menengah Atas Negeri II Pujud (SMAN2), dimana disini juga memiliki tempat yang strategis untuk di bangun sebuah warnet. Karena memudahkan bagi siswa siswi untuk membuat tugas dan menerapkan ilmu pada bidang internet.
3. *Client 3* akan ditempatkan di perumahan penduduk, disini juga merupakan tempat yang memiliki potensi untuk dibangun warnet. Karena memudahkan bagi masyarakat setempat untuk melakukan akses internet.

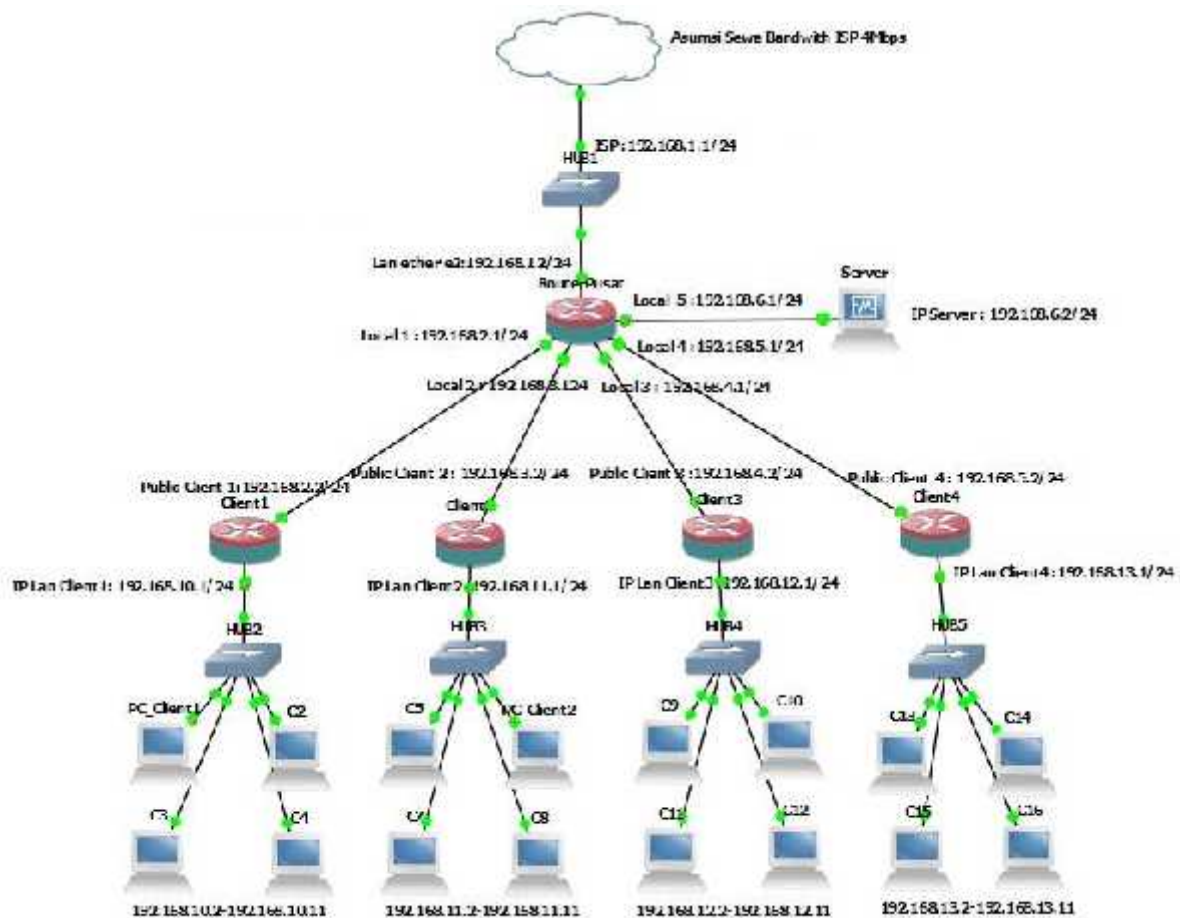
4. *Client 4* akan ditempatkan didekat kantor Camat Pujud dan Jalan lintas Pujud ke Rokan Hulu Riau, disini merupakan tempat yang memiliki potensi untuk dibangun tempat umum untuk mengakses internet.

3.4.2 Perencanaan Rute Jaringan VPN

Jarak setiap warnet antara *Server* VPN untuk *Client 1* yaitu di dekat PT. Tunggal Mitra yang dalam perencanaannya jarak antara *Server* VPN ± 5 km, untuk *Client 2* yaitu di dekat SMAN2 Pujud yang dalam perencanaannya jarak antara *Server* VPN ± 2 km, untuk *Client 3* yaitu di dekat perumahan penduduk jarak antara *Server* VPN ± 3 km, dan untuk *Client 4* yaitu di dekat kantor Camat dan Jalan lintas Pujud ke Rokan Hulu Riau jarak antara *Server* VPN ± 6 km. Serta untuk *Server* VPN dari desa Pujud Rokan Hilir Riau ke Kota Bagan Batu yang berjarak dari ISP ± 150 km untuk penyewaan *bandwidth*.

3.5 Topologi Jaringan

Topologi dalam perencanaan jaringan IP VPN nantinya menggunakan topologi *star*. Berikut topologi VPN dengan koneksi intranet dapat dilihat pada Gambar 3.3 berikut :



Gambar 3.3 Topologi VPN intranet

Adapun susunan IP address VPN Intranet dari topologi jaringan di atas dapat dilihat pada Tabel 3.1 berikut.

Tabel 3.1 Susunan IP Address pada perencanaan Topologi Jaringan VPN

Jenis	IP Address	Subnet Mask	Fungsi
ISP Publik	192.168.1.1	255.255.255.0	Alamat IP Publik dari <i>Internet Service Provider</i> (ISP)
Gateway Server VPN	192.168.1.2	255.255.255.0	Sebagai alamat <i>gateway Router Mikrotik Server VPN</i>
IP lokal	192.168.2.1	255.255.255.0	Sebagai IP Lokal untuk menghubungkan <i>Router Mikrotik pusat VPN ke Router Mikrotik Client 1</i>
Gateway Server VPN	192.168.2.2	255.255.255.0	Sebagai IP <i>gateway Router Mikrotik Client 1</i>
IP lokal	192.168.3.1	255.255.255.0	Sebagai IP Lokal untuk menghubungkan <i>Router Mikrotik pusat VPN ke Router Mikrotik Client 2</i>
Gateway Server VPN	192.168.3.2	255.255.255.0	Sebagai IP <i>gateway Router Mikrotik Client 2</i>
IP lokal	192.168.4.1	255.255.255.0	Sebagai IP Lokal untuk menghubungkan <i>Router Mikrotik pusat VPN ke Router Mikrotik Client 3</i>
Gateway Server VPN	192.168.4.2	255.255.255.0	Sebagai IP <i>gateway Router Mikrotik Client 3</i>
IP lokal	192.168.5.1	255.255.255.0	Sebagai IP Lokal untuk menghubungkan <i>Router Mikrotik pusat VPN ke Router Mikrotik Client 4</i>
Gateway Server VPN	192.168.5.2	255.255.255.0	Sebagai IP <i>gateway Router Mikrotik Client 4</i>
IP lokal	192.168.6.1	255.255.255.0	Sebagai IP Lokal untuk menghubungkan <i>Router Mikrotik pusat VPN ke PC Server</i>
IP PC Server	192.168.6.2	255.255.255.0	Sebagai IP LAN PC Server
IP PC Client1	192.168.10.2	255.255.255.0	Sebagai IP LAN PC Client1
IP PC Client2	192.168.11.2	255.255.255.0	Sebagai IP LAN PC Client2
IP PC Client3	192.168.12.2	255.255.255.0	Sebagai IP LAN PC Client3
IP PC Client4	192.168.13.2	255.255.255.0	Sebagai IP LAN PC Client4
IP VPN	192.168.6.5	255.255.255.0	Sebagai IP untuk Jalur <i>tunneling VPN client 1</i>
IP VPN	192.168.6.6	255.255.255.0	Sebagai IP untuk Jalur <i>tunneling VPN client 2</i>
IP VPN	192.168.6.7	255.255.255.0	Sebagai IP untuk Jalur <i>tunneling VPN client 3</i>
IP VPN	192.168.6.8	255.255.255.0	Sebagai IP untuk Jalur <i>tunneling VPN client 4</i>

3.6 Kapasitas Pengguna

Pada perencanaan jaringan IP VPN ini di gunakan *bandwidth* atau kapasitas pengguna untuk akses internet yaitu di asumsikan dari sebuah ISP sebesar 4 Mbps dan untuk masing masing *client* warnet nantinya akan didistribusikan sebesar 1 Mbps dan di konfigurasi manajemen *bandwidth*nya. Asumsi perhitungan *bandwidth* yang berdasarkan lokasi perencanaan warung internet di Desa Pujud dalam penelitian ini adalah:

1. Warnet pertama yaitu di dekat PT. Tunggal Mitra yang sesuai kondisi disini para pelanggannya para karyawan PT. Tunggal Mitra sehingga dalam pemakaiannya diperkirakan hanya *browshing*, *download*, dan *upload*. Berdasarkan data dilapangan dapat dihitung asumsi penggunaan *bandwidth* bahwa 35% akses untuk *browshing*, 40% untuk *download* dan 25% untuk *upload*. Maka harus disediakan minimum $35\% \times 1 \text{ Mbps} = 0,35 \text{ Mbps}$ untuk *browshing*, $40\% \times 1 \text{ Mbps} = 0,4 \text{ Mbps}$ untuk *download* dan $25\% \times 1 \text{ Mbps} = 0,25 \text{ Mbps}$ untuk *upload*.
2. Warnet kedua yaitu di dekat SMAN2 Pujud yang sesuai kondisi disini para pelanggan siswa siswi dalam pemakaian *bandwidth* cukup besar, diperkirakan pemakaian untuk game *online*, *browshing*, *download* dan *upload*. Berdasarkan data dilapangan dapat dihitung asumsi penggunaan *bandwidth* bahwa 50% akses untuk game online, 20% untuk *browshing*, 20% untuk *download* dan 10% untuk *upload*. Maka harus disediakan minimum $50\% \times 1 \text{ Mbps} = 0,5 \text{ Mbps}$ untuk game online, $20\% \times 1 \text{ Mbps} = 0,2 \text{ Mbps}$ untuk *browshing*, $20\% \times 1 \text{ Mbps} = 0,2 \text{ Mbps}$ untuk *download* dan $10\% \times 1 \text{ Mbps} = 0,1 \text{ Mbps}$ untuk *upload*.
3. Warnet ketiga yaitu di dekat perumahan penduduk yang sesuai kondisi disini para pelanggan masyarakat desa pujud sehingga dalam pemakaian diperkirakan hanya *browshing*, *download*, dan *upload*. Berdasarkan data dilapangan dapat dihitung asumsi penggunaan *bandwidth* bahwa 35% akses untuk *browshing*, 40% untuk *download* dan 25% untuk *upload*. Maka harus disediakan minimum $35\% \times 1 \text{ Mbps} = 0,35 \text{ Mbps}$ untuk *browshing*, $40\% \times 1 \text{ Mbps} = 0,4 \text{ Mbps}$ untuk *download* dan $25\% \times 1 \text{ Mbps} = 0,25 \text{ Mbps}$ untuk *upload*.
4. Warnet keempat yaitu di dekat kantor camat Pujud dan jalan lintas Pujud ke Rokan Hulu Riau yang sesuai kondisi disini para pelanggan para karyawan dan masyarakat setempat sehingga penggunaan diperkirakan hanya *browshing*, *download*, dan *upload*. Berdasarkan data dilapangan dapat dihitung asumsi penggunaan *bandwidth* bahwa

35% akses untuk *browsing*, 40% untuk *download* dan 25% untuk *upload*. Maka harus disediakan minimum $35\% \times 1 \text{ Mbps} = 0,35 \text{ Mbps}$ untuk *browsing*, $40\% \times 1 \text{ Mbps} = 0,4 \text{ Mbps}$ untuk *download* dan $25\% \times 1 \text{ Mbps} = 0,25 \text{ Mbps}$ untuk *upload*.

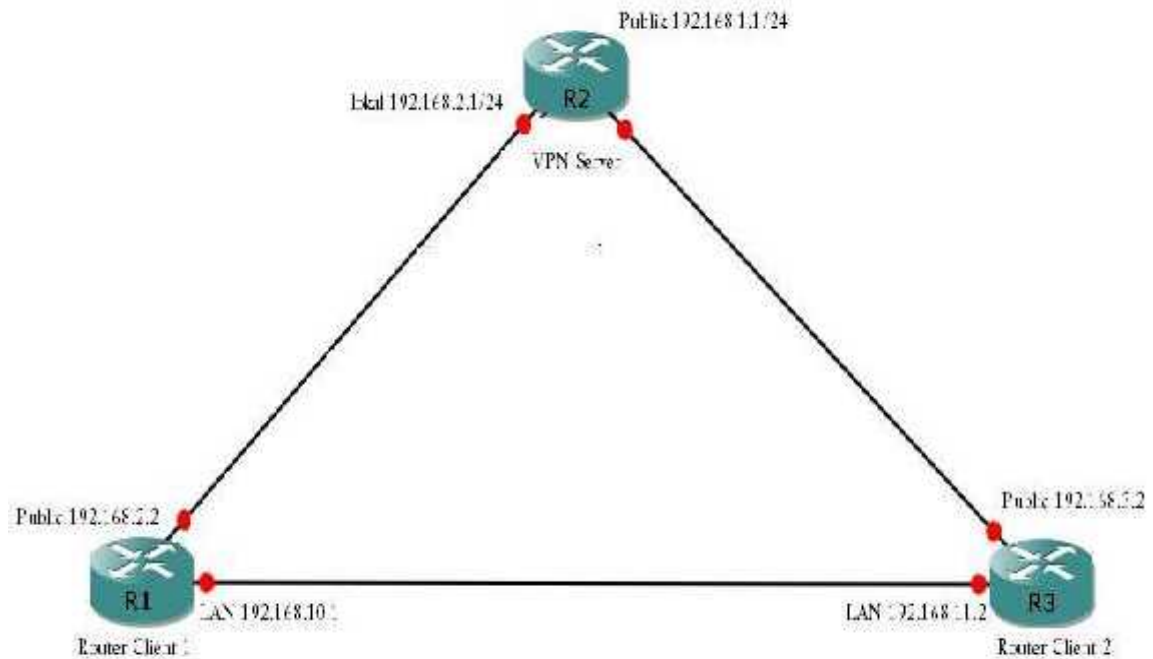
3.7 Perencanaan Simulasi

3.7.1 Perencanaan Sistem Berbasis IP VPN

Tahap pertama dalam perencanaan sistem ini adalah mengkonfigurasi Router Pusat yang bertugas sebagai *Server* yaitu melakukan alokasi *bandwidth* dari *Internet Service Provider* (ISP) untuk digunakan oleh *user*. Kemudian membuat konfigurasi VPN Pusat untuk *authentikasi* pengguna/*user* agar saling terhubung ke masing-masing *client* secara intranet. *Authentikasi user* digunakan dengan memakai *username* dan *Password* yang harus didaftarkan dahulu ke VPN Router Pusat sebagai syarat supaya *user* bisa terhubung ke server untuk mengakses data server dan memakai *bandwidth* yang telah dialokasikan, hanya *user* yang terdaftar di VPN Server yang dapat menggunakan *bandwidth*. Selain membuat VPN Server, juga harus membuat VPN gateway Server yang menghubungkan antara *user* dengan *internet* karena VPN hanya membuka akses/gerbang antara *user* dengan Server sebagai bukti bahwa *username* dan *Password* telah terdaftar di Server, untuk menghubungkan antara *user* dengan *internet* maka Server harus membuat gerbang VPN gateway yang dapat membuka gerbang antara *user* dengan *internet* sehingga *user* dapat mengakses *bandwidth* yang telah dialokasikan untuknya.

3.7.2 Menggunakan Mikrotik RouterOS Sebagai Network Manajemen Bandwithnya

Penelitian ini menggunakan Mikrotik RouterOS dalam perencanaan jaringan karena Mikrotik RouterOS memiliki berbagai fitur dan tool, baik untuk jaringan kabel maupun *wireless* yang menjadikan komputer menjadi *router network* yang handal. Mikrotik RouterOS sekarang ini banyak digunakan oleh ISP, *provider hotspot*, ataupun oleh pemilik warnet. Gambaran rencana arsitektur jaringan dalam penelitian ini sebagaimana terlihat dalam Gambar 3.4 bahwa VPN ini akan menghubungkan dari VPN Mikrotik kepada *Router Client 1* dan *Router Client 2*. Kedua titik ini bisa disalurkan melalui jalur menggunakan *access point* maupun kabel.

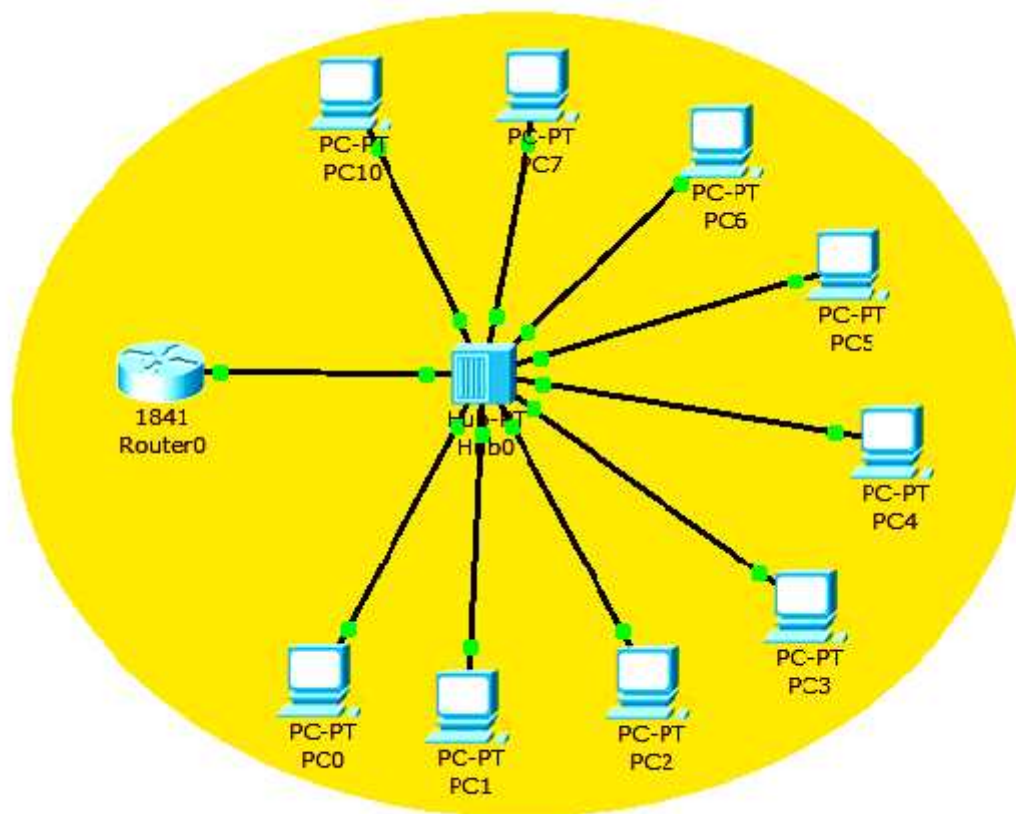


Gambar 3.4. arsitektur jaringan *Router VPN*

Dimulai dari *user* yang akan terhubung dengan koneksi Internet. Setelah itu *user* akan mengakses *interface* awal baik itu *games* maupun *browser* yang kemudian sistem akan melakukan pengecekan *IP Address* yang berfungsi untuk mengecek *IP Address* tersebut masuk. Ketika pengecekan *IP Address* selesai maka *IP Address* tersebut sudah dikenakan aturan tentang besaran *bandwidth* yang dapat digunakan oleh *IP Address* tersebut.

3.7.3 Perencanaan Warung Internet *Client*

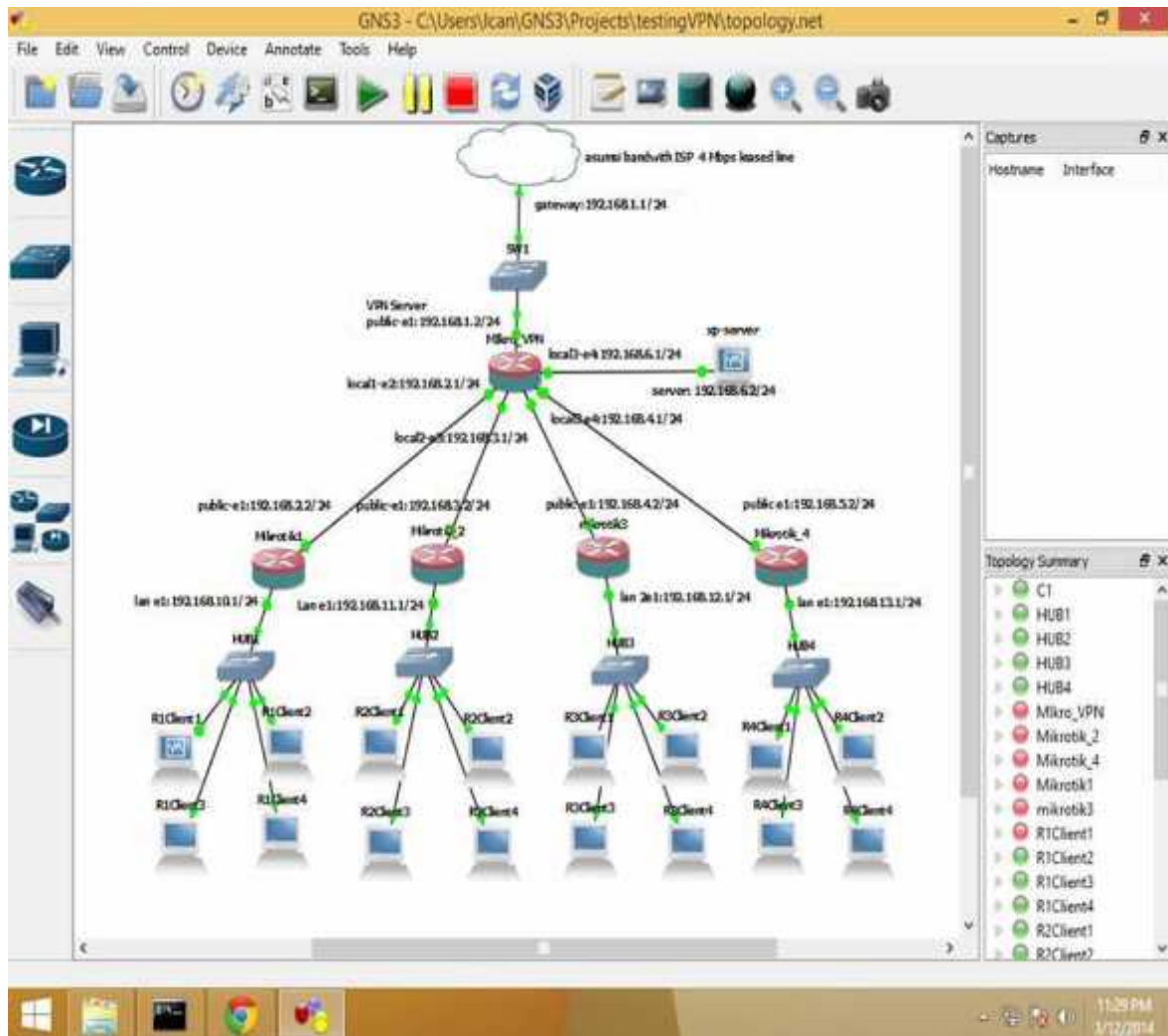
Jaringan yang akan direncanakan dengan memperhatikan konfigurasi minimal dari perencanaan warnet *client* menggunakan *bandwidth* 1 Mbps didistribusikan untuk 10 PC. Maka bila dibagi untuk 10 PC akan menjadi 100 Kbps, dimana 1 Mbps ini merupakan titik efektif untuk penggunaan akses internet pada *Client* warnet sejumlah 10 PC. Selain itu pertimbangan ekonomis harga *bandwidth* yang masih relatif terjangkau untuk 1 Mbps. Bila pada perkembangan selanjutnya *bandwidth* berubah maka tidak berpengaruh dalam mencapai tujuan dari penelitian. Karena penelitian ini adalah untuk langkah awal dalam efisiensi akses koneksi internet untuk warnet-warnet di desa Pujud Rokan Hilir Riau. Untuk perencanaan warnet client dapat di lihat pada Gambar 3.5 berikut.



Gambar 3.5 perencanaan Warnet *Client* untuk 10 PC

3.7.4 Model jaringan pada *Graphical Network Simulator* (GNS3)

Pada penelitian ini, penulis merencanakan model jaringan *Internet Protocol Virtual Private Network* (IP VPN) dan *Network Management* menggunakan sistem Intranet. Model jaringan dimodelkan dengan menggunakan *software* simulasi *Graphical Network Simulator* (GNS3). Setelah itu model jaringan tersebut disimulasikan dengan menggunakan *software Graphical Network Simulator* (GNS3) juga. Penelitian ini dilakukan untuk mendapatkan model jaringan IP VPN dan *Network Management* menggunakan Mikrotik RouterOS sebagai manajemen bandwithnya. Model jaringan tersebut diharapkan nantinya siap untuk diimplementasikan di lapangan. Progress perencanaan jaringan pada *software* GNS3 dapat di lihat pada Gambar 3.6 berikut.



Gambar 3.6 *Progress Perencanaan Internet Protocol Virtual Private Network (IP VPN) dan Network Management untuk Efisiensi Koneksi Internet dengan Sistem Intranet*

Keterangan dari gambar 3.6 *progress* perencanaan *internet protocol virtual private network* (IP VPN) dan *Network Management* untuk Efisiensi Koneksi Internet dengan Sistem Intranet sebagai berikut :

1. *Cloud 1 (C1)* digunakan sebagai ISP yang terhubung ke sebuah *localhost* PC yang dibuat secara manual melalui *microsoft loop adapter* .
2. *Router Server VPN (RVPN)* digunakan sebagai induk dari semua *Router* yang terhubung. *Server VPN* ini bertugas menangani pengolahan, pendistribusian data dan manajemen bandwidth secara terpusat, juga sebagai pintu gerbang menuju internet (*gateway*). Sehingga RVPN menjadi koordinator pada sistem jaringan IP VPN.

3. *Router 1* digunakan sebagai *Client 1* dari sebuah jaringan VPN yang terhubung melalui *Router Server VPN*. dan berfungsi sebagai induk dari *PC Client* yang bertugas menangani *sharing* data, manajemen bandwidth ke PC warnet.
4. *Router 2* digunakan sebagai *Client 2* dari sebuah jaringan VPN yang terhubung melalui *Router Server VPN*. dan berfungsi sebagai induk dari *PC Client* yang bertugas menangani *sharing* data, manajemen bandwidth ke PC warnet.
5. *Router 3* berfungsi sama dengan *Router 1* dan *2* yaitu digunakan sebagai *Client 3* dari sebuah jaringan VPN yang terhubung melalui *Router Server VPN*. dan berfungsi sebagai induk dari warnet *Client 3* yang bertugas menangani *sharing* data, manajemen bandwidth ke PC dan menjadi koordinator pada sistem jaringan warnet.
6. *Router 4* berfungsi sama dengan *Router 1*, *2*, dan *3* yaitu digunakan sebagai *Client 4* dari sebuah jaringan VPN yang terhubung melalui *Router Server VPN*. dan berfungsi sebagai induk dari warnet *Client 4* yang bertugas menangani *sharing* data, manajemen bandwidth ke PC dan menjadi koordinator pada sistem jaringan warnet.
7. HUB 1 digunakan sebagai penghubung dari *Router Client 1* ke PC warnet. Karena HUB berfungsi menghubungkan peralatan-peralatan dengan *ethernet* untuk menjadikannya dalam satu segmen jaringan. Begitu juga dengan HUB 2, HUB 3 dan HUB 4.

3.7.5 Konfigurasi

a. Konfigurasi *Router VPN Server*

Gateway (ISP)= 192.168.1.101

b. Mengganti nama *Router*

```
[admin@MikroTik]> /system identity edit name;
```

Edit menjadi “RVPN”, tekan Ctrl+o

```
[admin@RVPN]> /system identity print
```

c. Mengganti nama *Ethernet* pada *Router VPN Server (RVPN)*

```
[admin@RVNP]> interface ethernet set ether1 name=public
```

```
[admin@RVPN]> interface ethernet set ether2 name=local1
```

```
[admin@RVPN]> interface ethernet set ether3 name=local2
```

```
[admin@RVPN]> interface ethernet set ether4 name=local3
```

d. Memberi IP Address *Router VPN Server (RVPN)*

```
[admin@RVPN]> ip address add address=192.168.1.102/24 interface=public
```

```
[admin@RVPN]> ip address add address=192.168.2.1/24 interface=local1
```

```
[admin@RVPN]> ip address add address=192.168.3.1/24 interface=local2
```

```
[admin@RVPN]> ip address add address=192.168.4.1/24 interface=local3
```

e. Konfigurasi Gateway Router VPN (RVPN)

```
[admin@RVPN]> ip route add dst-address=0.0.0.0/0 gateway= 192.168.1.101
```

f. Konfigurasi DNS Server Router VPN (RVPN)

```
[admin@RVPN]>ip dns set servers=192.168.1.101 allow=remote-requests=yes
```

Pada tahap ini *Router* sudah terkoneksi dengan internet, lakukan test ping google

```
[admin@RVPN]>ping www.google.com
```

g. Pembagian Bandwith

Bandwith dibagi pada *Router 1, Router 2, Router 3*. Berikut konfigurasinya dengan *Console*:

```
[admin@RVPN]>/queue simple add name="R1" target-address=192.168.2.2 max-  
limit=64/128k
```

```
[admin@RVPN]>/queue simple add name="R2" target-address=192.168.3.2 max-  
limit=64/128k
```

```
[admin@RVPN]>/queue simple add name="R3" target-address=192.168.4.2 max-  
limit=64/128k
```

Untuk melihat pembagian bandwith :

```
[admin@RVPN]> /queue simple print
```

h. Konfigurasi Router 1 (R1)

➤ **Mengganti nama *Router***

```
[admin@MikroTik]> /system identity edit name;
```

Edit menjadi "R1", tekan Ctrl+O

```
[admin@R1]> /system identity print
```

➤ **Mengganti nama *Ethernet Router R1***

```
[admin@R1]> interface ethernet set ether1 name=public
```

```
[admin@R1]> interface ethernet set ether2 name=lan
```

➤ **Memberi IP Address**

```
[admin@R1]> ip address add address=192.168.2.2/24 interface=public
```

```
[admin@R1]> ip address add address=192.168.10.1/24 interface=lan
```

➤ **Konfigurasi Gateway R1**

```
[admin@R1]> ip route add dst-address=0.0.0.0/0 gateway= 192.168.2.1
```

➤ **Melihat ip route**

```
[admin@RVPN]> ip route print
```

i. Konfigurasi DNS Server

```
[admin@R1]>ip dns set servers=192.168.2.1 allow-remote-requests=yes
```

j. Konfigurasi NAT

```
[admin@RVPN]>ip firewall nat add chain=srcnat out-interface=public  
action=masquerade
```

k. DHCP Server

```
[admin@R1]>/ip pool add name=pool1 ranges=192.168.10.2-192.168.10.254
```

```
[admin@R1]>/ip dhcp-server add name=server1 address-pool=pool1 interface=lan
```

```
[admin@R1]>/ip dhcp-server network add address=192.168.10.0/24
```

```
gateway=192.168.10.1 dns-server=192.168.1.101
```

3.8 Uji koneksi

Pada tahap pengujian koneksi ini merupakan sebagai langkah pengujian dari hasil perancangan sistem VPN yang telah dilakukan. Pengujian dapat dilakukan dengan melakukan prosedur sebagai berikut.

1. *Traceroute* dari PC Server VPN ke PC Client 1, Client 2, Client 3, dan Client 4. Langkah ini akan menghasilkan alur rute alamat IP PC Server VPN dan sebaliknya.
2. Ping dari VPN Client Router ke VPN Server Gateway dan sebaliknya. Langkah ini akan menghasilkan nilai *round trip time* dan *packet loss*.
3. Pengujian koneksi *Remote Desktop* dari PC Server VPN ke PC Client 1, Client 2, Client 3, dan Client 4. Pengujian ini berupa pengiriman data melalui jaringan VPN yang telah dirancang.
4. Pengujian FTP (*File Transfer Protocol*) transfer. Pengujian ini berupa uji pengunduhan (*download*) dari FTP Server VPN ke PC VPN Client. Lalu uji pengunggahan (*upload*) dari PC VPN Client ke FTP Server VPN. Pengamatan dilakukan pada koneksi VPN Client ke VPN Gateway dengan memperhatikan *packet loss* dan *round trip time* serta lama durasi transfernya.

3.9 Analisis

Menguraikan dan menganalisa secara keseluruhan semua yang telah dihasilkan dan telah diolah pada Bab IV tentang Perencanaan Jaringan *Internet Protocol Virtual Private Network* (IP VPN) dan *Network Management* untuk Efisiensi Koneksi Internet dengan Sistem Intranet.

3.10 Penutup

Menguraikan secara singkat mengenai kesimpulan dan saran dari penelitian dan penulisan tugas akhir.